427. For example, FB gave Amazon extended unfettered access to FB user' information because it was spending money on FB advertising and partnering with FB on the launch of its "Fire" smartphone.

428. FB also discussed cutting off unfettered access to FB user' information for a messaging application that was viewed by FB executives as a too popular competitor.

429. Private communication between users is "increasingly important," Zuckerberg said in a 2014 *New York Times* interview. "Anything we can do that makes people feel more comfortable is really good." But leaked FB documents show that secretly, contrary to FB's public statements, FB conjured up ways to require third party applications to compensate FB for unfettered access to its FB user's information, including direct payment, advertising spending and information-sharing arrangements.

430. Ultimately FB decided not to sell the information directly but rather to dole it out to application developers who were considered personal friends of Zuckerberg and/or Sandberg or who spent big money on FB ads like Amazon and/or shared their own customer information with FB.

431. About 400 of the 4,000 leaked FB pages of the leaked documents had been previously been disclosed. However, the previously undisclosed leaked documents convey the most comprehensive insight into FB's deceptive and unlawful activities while the company struggled to adapt to the rise of smartphones following its scratchy debut as a public company in 2012.

432. The thousands of previously undisclosed FB leaked documents were anonymously leaked to the British investigative journalist Duncan Campbell, who shared them with a handful of media organizations such as *NBC News, Computer Weekly* and *Süddeutsche Zeitung*.

433. FB has not questioned the authenticity of the leaked FB documents, each of which was presented as evidence in a California court case between FB and a startup company called Six4Three that sued FB in 2015 after FB announced plans to cut off their unfettered access to FB user' information.

434. The Six4Three's computer application, called Pikinis, was launched in 2013 and relied on FB user' information to find photos of persons clothed only in bathing suits.

435. According to the *Wall Street Journal*, FB has admitted that it considered charging for unfettered access to FB user' information, but found there were better ways to monetize unfettered access to its users' information.

436. In a preliminary decision, the judge in the Six4Three case found "evidence of FB's fraudulent conduct.

437. The leaked documents show that FB's plans to sell unfettered access to FB user' information received support from FB's most senior executives, including CEO Zuckerberg, COO Sheryl Sandberg, Chief Product Officer Chris Cox and Vice President of growth Javier Olivan.

438. When in 2015 FB discontinued unfettered access to FB user' information for certain third parties, that FB action contributed to the decline of Pikinis, Lulu, and Beehive .

439. One of the most striking examples of FB's willful misconduct to emerge from the leaked documents is the way that FB user' information was traded to squeeze money or shared information from third party application developers.

440. In the wake of the Cambridge Analytica scandal and rising awareness of the Six4Three lawsuit, FB attempted to spin the modest changes it made to its platform in 2014 and 2015 as major events and as being driven by FB concerns over user privacy.

441. However, the leaked documents show that protecting FB user' privacy was not a major concern for FB, and the issue was rarely discussed in the thousands of pages of leaked emails and meeting summaries.

442. When FB user' privacy was mentioned, it was in the context of how FB can use it as a public relations strategy to soften the blow of the sweeping changes to application developer's unfettered access to FB user' information. The leaked documents include several examples suggesting that these changes were designed to cement FB's power in the marketplace, not to protect users.

443. Early on, FB recognized that working with and helping third party application developers with free unfettered access to FB user' information, would make FB more interesting and accelerate FB's growth.

444. Beginning in early 2010, FB created tools that allowed makers of computer games and other applications to connect with FB users so that FB users would spend more time using the FB platform and managed to achieve this through its Graph API (Application Programming Interface) that allowed software programs to interact with each other.

445. In FB's case, this meant that third party applications such as online computer games could post updates on FB user' profiles, which would be seen by computer game player's FB "Friends" and tempt them to play as well and allow game creators to access information from FB users, including their connections to FB "Friends," FB "Likes," locations, updates, photos and more.

446. Graph API, and particularly the way it let third parties promote their products and extract information from a FB user's "Friends," was a key feature of FB that Six4Three and thousands of other companies relied upon.

447. However, a few years later, FB decided the application developers were getting more value from their unfettered access to FB user' information than FB was getting from the application developers.

448. Soon after FB sold a wee portion of its stock to the public, the rapid growth of the cellphones threatened FB's market power and growth and an internal FB presentation looking back at this period used the phrase "terminal decline" to describe the fall in FB user engagement.

449. Zuckerberg, Sandberg and other FB executives spent months brainstorming ways to exploit the explosive growth of cellphone use before that explosively expanding market got away from them.

450. One idea that FB kept returning to was to make money from FB's application developer partners by charging them for unfettered access to FB's users and their information.

451. Several proposals for charging application developers for unfettered access to FB's platform and FB user information were put forward in a presentation to the company's board of directors.

452. Among the suggestions: a fixed annual fee for application developers for reviewing their applications; an access fee for applications that requested FB user' information; and a charge for "premium" unfettered access to FB user' information, such as a user trust score or a ranking of the strongest relationships between FB users and their FB "Friends."

453. "Today the fundamental trade is 'information for distribution,' whereas we want to change it to either 'information for $' and/or '$ for distribution,'" a FB business development director wrote in an August 2012 internal email.

454. Such discussions continued through October 2012, when Zuckerberg explained to close friend Sam Lessin the importance of controlling third party application's ability to access FB's user' information and reach FB user's "Friends" on the FB platform.

455. Without that leverage, "I don't think we have any way to get application developers to pay us at all," Zuckerberg wrote in an email to Lessin.

456. Then Zuckerberg suggested pursuing 100 deals with application developers "as a path to figuring out the real market value of FB user' information and then setting a public rate for application developers. "The goal here wouldn't be the deals themselves," said Zuckerberg, "…but that through the process of negotiating with them we'd learn what application developers would actually pay, which might be different from what they'd say if we just asked them about the value, and then we'd be better informed on our path to set a public rate."

457. As usual, Zuckerberg ignored the potential privacy risks associated with FB's user information-sharing arrangements. "I'm generally skeptical that there is as much information leak strategic risk as you think," he wrote in the email to Lessin. "I think we leak info to developers, but I just can't think of any instances where that information has leaked from developer to developer and caused a real issue for us." But, the following year, a privacy defect affecting a third party application developers created precisely that sort of issue for FB, as depicted in a panicky chatlog between Michael Vernal, who was FB's director of engineering, and other senior FB employees.

458. Apparently, Zuckerberg's private communications were leaked from FB to an external application in an unexpected way.

459. Vernal said that it could have been near-fatal for the FB if Zuckerberg had accidentally disclosed earnings ahead of time because a FB sanctioned application had intruded on his privacy.

460. "Holy crap," replied Avichal Garg, then director of product management. "DO NOT REPEAT THIS STORY OFF OF THIS THREAD," added Vernal. "I can't tell you how terrible this would have been for all of us had this not been caught quickly."

461. In late November 2012, Zuckerberg sent a long email to FB's senior executives stating FB should not charge application developers for unfettered access to FB user' information.

462. However, Zuckerberg also said that unfettered access to FB user' information should be contingent on the application developers sharing all of the "social content" generated by their applications with FB, something Zuckerberg called "full reciprocity."

463. The existing arrangement, where application developers weren't required to share their information with FB, might be "good for the world, but it's not "good for us," Zuckerberg wrote in an email and added that "…though FB could charge application developers to access FB user' information, FB stood to benefit more from requiring application developers to compensate FB by sharing their customer information and by buying advertising on FB's platform.

464. FB began making deals with some of its most valued partners, including dozens of application developer friends of Zuckerberg and Sandberg by "whitelisting" their

unfettered access to FB user' information while restricting unfettered access to application developers FB determined were competitors.

465. These FB negotiated information access deals with key FB business partners, including Tinder, Sony, Amazon and Microsoft, required sweeping changes to the FB platform, changes FB planned to announce at its annual application developer conference in April 2014.

466. in June 2013I, leaked FB documents described that Amazon received special treatment for the launch of a group gifting product, despite the fact that it competed with one of FB's own products.

467. "Remind me, why did we allow them [Amazon] to do this? Do we receive any cut of purchases?" Chris Daniels, then FB's director of business development, asked in an email.

468. "No, but Amazon is an advertiser and supporting this with advertisements ... and working with us on deeper integrations for the Fire," Amazon's smartphone, replied Jackie Chang, who worked with FB's strategic business partners.

469. Amazon released a statement to *NBC News*: "Amazon uses publicly available APIs provided by FB in order to enable FB experiences for our products and only uses information in accordance with our privacy policy." An admission that Amazon had collected and stored FB user' information for its own use and profit and that that information was now subject to Amazon's customer information policies.

470. The applications of application developers that were not considered "strategic partners" got less favorite nation status treatment from FB.

471. In a March 2013 discussion, Justin Osofsky, then director of FB platform business partnerships, described restricting the MessageMe application from unfettered access to FB user' information because it had grown too popular and could compete with FB messages.

472. Osofsky asked his staff to see if any other messenger applications have "hit the growth team's radar recently." "If so, we'd like to restrict them at the same time to group this into one press cycle," he wrote in an email.

473. The FB driven deal negotiations created confusion among FB's business partners who had grown accustomed to unfettered access to FB user' information.

474. "We gave a bunch of stuff for free historically (information, distribution) and now we're making you 'pay' for it via reciprocal value," Vernal, director of FB engineering, wrote in an email in June 2013. He added, "The confusing thing here is that we haven't really announced these changes publicly/broadly yet."

475. Some FB employees were unhappy about this direction, particularly the way FB appeared to be blocking competitors from unfettered access to FB user' information.

476. Following is an extract from a December 2013 chatlog between several FB senior engineers talking about the changes to application developers' unfettered access to FB user' information:

477. Bryan Klimt: "So we are literally going to group applications into buckets based on how scared we are of them and give them different APIs? ... So, the message is, 'if you're going to compete with us at all, make sure you don't integrate with us at all'? I'm just dumbfounded."

478. Kevin Lacker: "Yeah this is complicated."

479. David Poll: "More than complicated, it's sort of unethical."

480. When it came to announcing the sweeping changes at FB's annual F8 application developer conference in April 2014, members of the communications team worked with Zuckerberg to craft a narrative around FB user' trust, not competition or profitability.

481. In a March 2014 email discussing Zuckerberg's keynote speech at FB's annual F8 application developer conference, where he was due to announce the removal of application developer's unfettered access to FB "Friends"' information, Jonny Thaw, a FB director of communications, wrote that it "may be a tough message for some application developers as it may inhibit their growth."

482. One idea that came up was talking in the keynote about some of the trust changes we're making on FB itself. So, the message would be: 'trust is really important to us, on FB we're doing A, B and C to help people control and understand what they're sharing and with platform applications we're doing D, E and F. If that doesn't work," he added, "we could announce some of FB's trust initiatives in the run up to F8 to make the changes for application developers seem more natural."

483. FB user trust was crucial when Zuckerberg delivered his keynote speech at the F8 conference on April 30, 2014, where Zuckerberg said: "Over the years, one of the things we've heard over and over again is that people want more control over how they share their information, especially with applications, and they want more say and control over how applications use their information," he told the audience of journalists and application developers. "And we take this really seriously because if people don't have the tools they need to feel comfortable using your applications, that's bad for them and that's bad for you."

484. But despite FB's purported focus on user privacy, FB staff member emails described confusion over the way third party applications could override user's privacy settings.

485. Even if FB users locked down their account so that their photos and other FB user' information were visible to "only me," those photos were still accessible by third parties.

486. In April 2015, Connie Yang, a FB product designer, told her colleagues that she'd discovered applications collecting FB profile information she had marked as "only me" and displaying it to "both you and other people using that application."

487. Even though FB eventually decided against charging application developers directly for unfettered access to FB user' information, one of the biggest threats FB now faced was not competition from application developers, but rather from federal antitrust regulation.

488. Eventually, the FTC announced a task force to monitor anti-competitive behavior in the technology industry to, in the words of FTC chair Joseph Simons, "…ensure consumers benefit from free and fair competition."

489. Congressional lawmakers started pressuring the FTC to investigate FB for antitrust violations.

490. David Cicilline, chairman of the House Judiciary Antitrust Subcommittee, wrote in a *New York Times* op-ed: ."FB appears to have used its [market] dominance to cripple other competitive threats by cutting them off from its massive network."

491. Trying to appease Congress and the FTC, a Zuckerberg op-ed appeared in the *Washington Post* in March 2018 calling for some regulation in such areas as election sabotage, but not antitrust punishment.

492. Ashkan Soltani, a privacy expert and former FTC chief technologist, said that Zuckerberg is approaching the looming threat of regulation with "bravado" and trying to "leverage things for his benefit."

493. Zuckerberg and other senior FB executives are now being investigated by Congress, governmental regulators and prosecutors domestic and foreign, as well as defending against numerous private party information privacy violation lawsuits.

494. In 2018, Zuckerberg told Congress that he's responsible for what happens at FB.

495. Senator Richard Blumenthal, who recently criticized the FTC for taking too long on the FB probe, wants the FTC to hold Zuckerberg accountable.

496. But Zuckerberg is accountable to no person and no government regulatory agency. His power over what FB does and doesn't do is absolute.

497. In late May 2019, FB investors voted overwhelmingly in support of proposals to fire Zuckerberg as chairman and scrap the firm's stock share structure. According to the results of votes at FB's annual shareholder meeting 68% of outside investors want the company to hire an independent chairman, up from 51% in 2018.

498. Despite the vote, the management and share restructuring proposals did not pass because of Zuckerberg has voting control by virtue of his majority stock holdings, which means he can and does ignore outside shareholder demands.

499. "Arrogance is not a substitute for good corporate governance," said Michael Connor, who helped coordinate action among activist FB investors.

500. Senator Blumenthal told the *Washington Post*. "Holding Mark Zuckerberg and other top FB executives personally at fault and liable for further wrongdoing would send a powerful message to business leaders across the country: You [Zuckerberg] will pay a hefty price for skirting the law and deceiving consumers."

501. In 2018, in a purported act of contrition, Zuckerberg told the House Committee on Energy and Commerce: "But it's clear now we [FB executives] didn't do enough to prevent these tools [the FB platform and application and algorithms] from being used for harm as well. That goes for fake news, foreign interference in elections and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our

responsibility and that was a big mistake. It was my mistake, and I'm sorry. I started FB. I run it, and I'm responsible for what happens here [at FB]."

IX. RUSSIAN "ACTIVE MEASURES" DEPLOYED TO SABOTAGE THE 2016 U.S. PRESIDENTIAL ELECTIONS USING THE FB PLATFORM AS SET OUT IN THE SPECIAL COUNSEL'S REDACTED REPORT

502. Plaintiffs repeat and re-allege all preceding and following paragraphs as if fully set forth herein.\

503. The first form of Russian election sabotage came principally from the Russian Internet Research Agency (Russian IRA), an organization funded by Yevgeniy Viktorovich Prigozhin and companies he controlled, including Concord Management and Consulting LLC and Concord Catering (collectively "Concord").

504. The Russian IRA conducted election sabotage operations using the FB platform targeted at prospective U.S. voters in a successful effort to sow discord among them that resulted in in the successful sabotage of the U.S. 2016 presidential election cycle.

505. These operations constituted "active measures" *(aKTMBHbMie eporrprumul)*, a term that refers to operations conducted by Russian security services aimed at influencing the course of international affairs.

506. The Russian IRA and its employees began operations targeting the U.S. in 2014, possibly earlier.

507. Using fictitious U.S. personas, Russian IRA employees operated FB accounts and FB group pages with the intent to influence U.S. voters. These FB groups and FB

accounts, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. persons.

508. Multiple Russian IRA controlled FB groups and other Russian entities engaged in similar "active measures" election sabotage operations targeting prospective U.S. voters

509. Over time, these Russian IRA-controlled FB accounts and other Internet-based platforms became a means to reach ever larger U.S. audiences.

510. Also, Russian IRA employees travelled to the U.S. in mid-2014 on an intelligence-gathering mission to obtain information and photographs for use in their FB and other Internet-based platforms.

511. Russian IRA employees posted derogatory information about a number of political candidates in the 2016 U.S. presidential elections and in early to mid-2016 Russian IRA election sabotage operations included supporting the Trump Campaign and disparaging Secretary Clinton's campaign.

512. The Russian IRA made various expenditures to carry out their election sabotage activities, including buying political advertisements on FB and other social media using fictitious names of U.S. persons and entities.

513. Some Russian IRA employees posing as U.S. persons and without revealing their Russian association communicated electronically with Trump Campaign associates and with other political activists seeking to coordinate pro-Trump political activities.

514. By the end of the 2016 U.S. presidential elections the Russian IRA had reached millions of U.S. persons through their FB and other Internet-based platforms.

515. The Special Counsel's "active measures" investigation has resulted in criminal charges against 13 Russian nationals and three Russian entities, principally for conspiracy to defraud the U.S., in violation of 18 U.S.C. § 371. See Volume I, Section V.A, infra; Indictment, United *States. v. Internet Research Agency, et al.,* 1 :18-cr-32 (D.D.C. Feb. 16, 2018), Doc. I (Internet Research Agency Indictment).

516. In November 2017, a FB executive testified that FB had identified 470 Russian IRA-controlled FB accounts that collectively made 80,000 posts between January 2015 and August 2017.

517. FB estimated the Russian IRA reached as many as 126 million persons through its FB accounts.

518. In a hearing before the Senate Select Committee on Intelligence, Colin Stretch, FB's then General Counsel, estimated that roughly 29 million people were served content in their FB "News Feeds" directly from the Russian IRA's 80,000 posts over two years.

519. Russian IRA posts from these FB pages were also shared, liked, and followed by people on FB, and, as a result, three times more people were exposed to a story that originated from the Russian U.S. election sabotage operation.

520. FB has estimated that approximately 126 million people were served content from a FB pages associated with the Russian IRA at some point during the 2016 presidential election cycle.

521. The FB general counsel also testified that FB had identified 170 FB-owned Instagram accounts that posted approximately 120,000 pieces of content during the 2016

presidential election cycle but did not offer an estimate of the number of persons reached via FB-owned Instagram.

522. In 2016, Russian IRA employees claiming to be U.S. political activists and administrators of FB groups, recruited U.S. persons to hold signs in front of the White House.

523. In June 2014, four Russian IRA employees applied to the U.S. Department of State to enter the U.S. and lied about the purpose of their trip, claiming to be four "Friends" who had met at a party. Ultimately, two Russian IRA employees-Anna Bogacheva and Aleksandra Krylova-received visas and entered the U.S. on June 4, 2014.

524. Dozens of Russian IRA employees were responsible for operating accounts on FB and were referred to within the agency as "specialists."

525. Russian IRA's operations focused their election rigging efforts on FB, YouTube, and Twitter and later added specialists who operated on Tumblr and Instagram accounts.

526. The Russian IRA-controlled FB groups including "Secured Borders, " the groups "Being Patriotic," "Stop All Immigrants," "Secured Borders," and "Tea Party News"), "Black Matters," "Blacktivist, " "Don't Shoot Us," "LGBT United,") and "United Muslims of America."

527. Throughout 2016, Russian IRA accounts published an increasing number of materials supporting the Trump Campaign and opposing the Clinton Campaign.

528. For example, on May 31, 2016, the operational account "Matt Skiber" began to privately message dozens of pro-Trump FB groups asking them to help plan a pro-Trump rally near Trump Tower.

529. To reach ever larger U.S. audiences, the Russian IRA purchased advertisements from FB that promoted Russian IRA FB groups on the FB newsfeeds of U.S. FB users.

530. According to FB, the Russian IRA purchased over 3,500 advertisements, paying approximately $100,000, using U.S. currency and Russian rubles.

531. During the 2016 U.S. presidential campaign, numerous Russian IRA-purchased advertisements explicitly supporting or opposing a presidential candidate or promoting U.S. political rallies organized, in part, by the Russian IRA.

532. Starting as early as March 2016, the Russian IRA purchased advertisements on FB that overtly opposed the Clinton Campaign.

533. For example, on March 18, 2016, the Russian IRA purchased an advertisement depicting candidate Clinton in a caption that read in part, " If one day God lets this liar enter the White House as a president - that day would be a real national tragedy."

534. Similarly, on April 6, 2016, the Russian IRA purchased FB advertisements for its account "Black Matters" calling for a "flashmob" of U.S. persons to "take a photo with #HillaryClintonForPrison2016 or #nohillary2016."

535. Russian IRA-purchased FB advertisements referencing candidate Trump supported the Trump Campaign and disparaged Secretary Clinton's campaign.

536. The first known Russian IRA advertisement explicitly endorsing Trump was purchased on April 19, 2016.

537. The Russian IRA bought an advertisement for its FB-owned Instagram account "Tea Party News" asking U.S. persons to help them "make a patriotic team of young Trump supporters " by uploading photos with the hashtag "#KIDS4TRUMP."

538. In subsequent months, the Russian IRA purchased dozens of advertisements supporting the Trump Campaign, predominantly through the FB groups "Being Patriotic," "Stop All Invaders," and "Secured Borders."

539. Collectively, the Russian IRA's social media accounts reached hundreds-of millions of Americans.

540. Individual Russian IRA FB and other platforms attracted hundreds of thousands of followers.

541. For example, at the time they were deactivated by FB after the completion of the 2016 U.S. presidential cycle in mid-2017, the Russian IRA's "United Muslims of America" FB group had over 300,000 followers, the "Don't Shoot Us" FB group had over 250,000 followers, the "Being Patriotic" FB group had over 200,000 followers, and the "Secured Borders" FB group had over 130,000 followers.

542. Moreover, the Russian IRA organized and promoted political rallies inside the U.S. while posing as U.S. grassroots activists, using FB groups and to announce and promote the event.

543. The Russian IRA then sent a large number of direct messages to its FB followers asking them to attend the event. From those who responded with interest in attending, the Russian IRA then sought a U.S. person to serve as the event's coordinator. In most cases, the Russian IRA account operator would tell the U.S . person that they personally could not attend the event due to some preexisting conflict or because they were somewhere else in the U.S.

544. The Russian IRA then further promoted the event by contacting U.S. media about the event and directing them to speak with the coordinator.

545. After the event, the Russian IRA posted videos and photographs of the event to the Russian IRA 's FB accounts.

546. The Special Counsel's redacted report identified dozens of U.S. rallies organized by Russian IRA.

547. The earliest evidence of a rally was a "confederate rally" in November 2015.

548. The Russian IRA continued to organize rallies even after the 2016 U.S. presidential elections.

549. The Russian IRA recruited U.S. persons from across the political spectrum. For example, the Russian IRA targeted a number of black social justice activists.

550. The Russian IRA also recruited moderators of conservative Internet-based groups to promote IRA-generated content, as well as recruited individuals to perform political acts, such as walking around New York City dressed up as Santa Claus with a Trump mask.

551. As the Russian IRA's online audience became ever larger, they tracked U.S. persons with whom they communicated and had successfully tasked with tasks ran in from organizing rallies to taking pictures with certain political messages.

552. With regard to Russian IRA interactions and contacts with the Trump Campaign, the Special Counsel's investigation identified several forms of connections between the Russian IRA and members of the Trump Campaign and no similar connections with the Clinton Campaign.

553. For example, on multiple occasions, members and surrogates of the Trump Campaign promoted, typically by linking, retweeting , or similar methods of reposting pro-Trump or anti-Clinton content published by the Russian IRA through Russian IRA-controlled FB and other platforms.

554. Among the U.S. leaders of public opinion targeted by the Russian IRA were various members and surrogates of the Trump Campaign. In total, Trump Campaign affiliates promoted dozens of tweets, posts , and other political content created by the Russian IRA.

555. In sum, the Special Counsel's investigation established that Russia interfered in the 2016 presidential election through the "active measures" social media campaign carried out by the Russian IRA, an organization funded by Yevgeniy Viktorovich Prigozhin and companies that he controlled.

556. The Special Counsel's redacted report concluded that Prigozhin, his companies and Russian IRA employees violated U.S. law through these operations, principally by

undermining through deceptive acts the work of federal agencies charged with regulating foreign influence in U.S. elections.

557. Moreover, the full extent of FB's participation in the sabotage of the 2016 U.S. presidential elections is as yet unknowable as much of the FB participation has been heavily redacted in the version of the Special Counsel's report released for public consumption and certain aspects of the sabotage exceeded to boundaries set by the DOJ for investigation by the Special Counsel.

X. CAUSES OF ACTION

558. All of the following causes of action are lodged against each of the FB Defendants.

COUNT ONE-VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT

559. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

560. At all relevant times, FB Defendants, FB's Internet-based platform, FB user' information and FB servers were involved in interstate and foreign commerce and communication as covered by 18 U.S.C. § 1030(e)(2) and still are.

561. In direct violation of 18 U.S.C. § 1030, FB Defendants, the Trump Campaign, Cambridge Analytica, Robert Mercer and others willfully and with fraudulent intent used Plaintiff's plundered FB user' information and that of nearly a hundred million other FB users to successfully sabotage the 2016 U.S. presidential elections.

562. The specific FB user' information of Plaintiffs plundered by Cambridge Analytica has not as yet been disclosed by FB or Cambridge Analytica, but that information could have included, but was not necessarily limited to, Plaintiff's individual and company names and addresses, hometowns; birthdates; gender; family connections; educational achievements; email addresses; relationship statuses; work histories; interests; hobbies ;religious and political affiliations; phone numbers; dates and times of active sessions on FB; dates and times and titles of Plaintiff's FB ads; connections and communications with other FB users; attendance at events and social gatherings, stored credit/debit card information, Plaintiffs thousands of FB "Friends" and FB "groups" Plaintiffs belonged to; a list of Internet provider addresses Zimmerman used, posts and/or websites Zimmerman has liked, Google searches conducted Zimmerman and photographs and/or videos.

563. This plundering of Plaintiff's FB user information, and that of nearly a hundred million other FB users, was accomplished, in part, when Robert Mercer funded and then directed Cambridge Analytica to create individual FB user' voter profiles based on demographics, political attitudes, religion, sexual orientation and the like and then together with the Trump Campaign and Russian operatives bombarded prospective 2016 U.S. presidential election voters with pro-candidate Trump and anti-Secretary Clinton disinformation, misinformation, propagandistic political messaging and advertising using the FB platform without a single intervention by FB, even though FB were well aware of this unlawful activity.

564. Instead of blocking the unlawful conduct of the Trump Campaign, Mercer, Cambridge Analytica and Russian operatives, FB and Cambridge Analytica aided and abetted the unlawful conduct by assigning their personal to the Trump Campaign political information processing offices that were used to help that campaign successfully sabotage the 2016 U.S. presidential elections in violation of 18 U.S.C. § 1030(a)(6)(A).

565. Plaintiffs and many others suffered damage and loss and continue to suffer damage and loss as a consequence of FB Defendant's actions, including but not limited to the cost of investigating and responding to the unauthorized access and abuse of their FB user information and that of their "Friends" and therefore seek compensatory and other equitable relief under 18 U.S.C. § 1030(g).

566. As a direct and proximate result of the conduct of FB, Plaintiffs have sustained significant harm, entitling them to damages in an amount to be established at trial.

COUNT TWO-UNJUST ENRICHMENT

567. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

568. As alleged herein, FB have unjustly received and retained monetary benefits from Plaintiffs by way of its profiting from the use of their FB user' information under unjust circumstances, such that inequity has resulted.

569. By engaging in the conduct described in this Complaint, FB knowingly obtained benefits from Plaintiffs as alleged herein under circumstances such that it would be inequitable and unjust for FB to retain them.

570. More specifically, by engaging in the acts and failures to act described in this Complaint, FB have been knowingly enriched by the savings in costs that should have been reasonably expended to protect the privacy of Plaintiff's FB user' information and by a substantial increase in the share price of FB. See *Restatement (Third) of Restitution and Unjust Enrichment* § 39(1) (2011).

571. Moreover, FB have been enriched unjustly by the use of Plaintiff's information for its advertising business, and has profited greatly as a result, even though it did not protect this information as it had promised.

572. By engaging in the conduct described in this Complaint, FB have knowingly obtained benefits from or by way of Plaintiffs, including by way of the use of their information in the course of its business, especially its lucrative advertising business, under circumstances such that it would be inequitable and unjust for it to retain them.

573. Thus, FB will be unjustly enriched if they are permitted to retain the benefits derived from the unauthorized and impermissible gathering and sharing of Plaintiff's FB user' information by FB authorized and unauthorized third parties.

As a direct and proximate result of the conduct of FB Defendants Plaintiffs have sustained significant harm, entitling them to damages in an amount to be established at trial.

COUNT THREE-VIOLATIONS OF CONSTITUTIONAL RIGHTS

574. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

575. This case is likely one of the first filed in this Court that addresses the relationship between the First Amendment and the Internet-based FB communications platform.

576. A fundamental principle of the First Amendment is that all persons have unfettered access to places where they can speak and listen, and then, after reflection, speak and listen once more. A basic rule is that a street or a park is a quintessential forum for the exercise of First Amendment rights. See *Ward v. Rock Against Racism,* 491 U. S. 781, 796 (1989).

577. FB brags that it offers its users a free facility for communication of all kinds. See *Reno v. American Civil Liberties Union,* 521 U. S. 844, 868 (1997).

578. FB users can debate religion and politics with their friends and neighbors or share vacation photos. All fifty states, thousands of cities and towns, and almost every elected official have FB accounts.

579. The First Amendment of the U.S. Constitution and 42 U.S.C. § 1983 protects Zimmerman's freedom of speech and association and provide protection against political viewpoint discrimination in the unfettered access to and use of public spaces, quasi-public spaces, and limited public spaces, which includes the use of the FB platform.

580. The Fourth Amendment of the U.S. Constitution and 42 U.S.C. § 1983 protect Zimmerman's right to privacy. See Puckingham v. North Carolina

581. 42 U.S.C. § 1983 is enforceable against FB Defendants because FB provides to its users a public free speech forum of unequaled proportions and audience reach that make state fairs and parks seem negligible.

582. FB is also a quasi-state actor because it wields potent monopolistic and political powers and is currently getting ready to launch its own international currency.

583. The state constitutions of North Carolina and California also provide constitutional free speech and privacy protections equal to those provided by the U.S. Constitution.

584. FB Defendants are quasi-state actors because they regulate and control the FB platform that served Plaintiffs and at least a billion other FB users' as a public and private communications platform.

585. FB Defendants acted deceptively, willfully, recklessly and unlawfully, individually and in concert, directly and indirectly, and motivated by their greed and political ideologies, maliciously violated Zimmerman's constitutionally protected rights of free speech, free association and privacy as well as his right to participate in free and fair elections.

586. FB Defendants discriminated against Zimmerman by blocking his unfettered access to his FB accounts for no expressed substantive reason, thus unlawfully censoring Plaintiff's political messaging, disallowing Zimmerman's communications with his thousands of FB "Friends," thus denying Zimmerman his right to express and promote his political and non-political ideas and to otherwise advertise and market his political and non-political books and to his FB "Friends" and others.

587. FB has never expressed a compelling reason for its blocking of Zimmerman's use of his FB accounts that, before being blocked by FB, he used to communicate with his

thousands of FB "Friends" and to advertise his political viewpoints and political and non-political books and receive messages from his FB "Friends."

588. FB conducted these unconstitutional activities after repeatedly bragging publicly and privately, that its foundational mission is to enable the citizens of this planet to freely communicate with one another.

589. Treasonous and unconstitutional conduct against the U.S. and its citizens shall consist not only in levying conventional war against them, or in adhering to their enemies, but also in providing them aid and comfort as FB did when they facilitated the Russian cyberattack on the 2016 U.S. presidential elections.

590. Chapter 18 of the U.S.C. sets out the punishment for treasonous conduct: "Whoever, owing allegiance to the United States, levies war against them or adheres to their enemies, giving them aid and comfort within the United States or elsewhere, is guilty of treason and shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than $10,000; and shall be incapable of holding any public office in the United States."

591. Although the *U.S. Constitution* defines treasonous conduct narrowly, in *United States v. Burr,* 159 U.S. 78 (1895), U.S. Supreme Court Chief Justice John Marshall in delivering the Court's opinion regarded war as not an abstract term, and defined treasonous as an assemblage of people who intend to use actual force against the government, and/or adhering to enemies of the U.S. and/or by giving enemies of the U.S. aid and comfort.

592. Later, in *Cramer v. United States,*,325 U.S. 1 (1945) the U.S. Supreme Court made clear that the provision of "aid and comfort" has to consist of an affirmative act during war, such as the Russian launched cyberattack on the 2016 U.S. presidential election cycle as knowingly facilitated by FB and as described throughout this Complaint, which is the modern equivalent of conventional warfare.

593. Since at least 2014, Russian intelligence agents and operatives in concert with FB the Trump Campaign, Cambridge Analytica, Robert Mercer and others have been conducting malicious cyberwarfare against the U.S., and its citizens and still are.

594. That cyberwarfare shares the same ultimate objective as conventional warfare, namely, among other things, the destruction of our democracy and the rule of law.

595. As cyberwarfare is the functional equivalent of conventional warfare, the willful and reckless actions and inactions of FB Defendants in facilitating the cyberattacks on the 2016 U.S. presidential election cycle qualify as substantive, identifiable, treasonous actions because those actions "adhered to the enemy" by rendering Russia "aid and comfort," by willfully and for profit facilitating Russia's malicious cyberwarfare against the U.S. and the U.S. public, including Zimmerman.

596. Also, by failing to protect Zimmerman against and report the numerous willful invasions of Plaintiff's FB user' information, FB Defendants have violated Plaintiff's Fourth Amendment right to privacy.

597. The constitutions of California and North Carolina are also on point.

598. For example, California's *Constitution* at Article 1 *Declaration of Rights*: Section

1 establishes a citizen's privacy rights declaring: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Section 28, deals with victim's rights.

599. North Carolina's *Constitution* Article 1, Section 10 establishes the right to free elections.

600. At a minimum, unconstitutional, other unlawful and possibly treasonous conduct of FB caused Zimmerman to suffer losses of his reasonable expectation to exercise his constitutional and other rights and privileges using the FB platform.

601. Zuckerberg has admitted he and others at FB were aware of the spread of Russian propaganda on the FB platform and did nothing to prevent it, instead pocketing Russian rubles and other currency from to sale of advertising space to Russian operatives.

602. Zimmerman had a reasonable expectation to use his FB accounts, which prior to having his accounts blocked by FB, to communicate with thousands of his FB "Friends" and to promote and advertise his political viewpoints and political and non-political books and receive messages and book orders from his FB "Friends."

603. FB Defendants willfully and recklessly enabled the unfettered access to Plaintiff's FB user information and that of their FB "Friends" without any authorization from Plaintiff by numerous third parties using various computer applications and telephonic devices.

604. A massive public outcry followed the revelation of FB's unconstitutional and

other tortious practices that eventually led to multiple ongoing foreign and domestic investigations of FB by governmental regulators and legislators and numerous private lawsuits

605. Further, the extent of the authorized and unauthorized FB user' information plundered by third parties from Plaintiffs will never be fully known and can continue far into the future.

606. Plaintiffs were substantially harmed and will continue to be harmed by the FB facilitated intrusion into Zimmerman's private affairs as detailed throughout this Complaint and FB Defendants active participation in the successful sabotage of the 2016 U.S. presidential elections that enabled the illegitimate and unlawful election of Trump.

607. Based on FB's intentionally deceptive, willful, reckless and unlawful actions and inactions as set out throughout this Complaint, Plaintiffs seek injunctive relief in the form of: (1) A FB-funded investigation to identify every third party that has had unfettered access to Plaintiff's FB user information, and how those third parties gained that access and how they used Plaintiff's FB user information and the destruction of it;
(2) certification by FB that no third parties are currently able to access Plaintiff's FB user information from FB's information files and those of third parties that obtained it from FB; and (3) destruction by FB of all of Plaintiff's FB user information now in FB and third party information files.

608. The cyber-sabotage of elections by saboteurs deploying various cyberweapons is a relatively new phenomena and primarily engaged in by well-heeled organizations and

persons like, as here, the Trump Campaign, FB, Russian intelligence agents and operatives and right-wing billionaires like Robert Mercer seeking to enrich themselves, grow their political power, undermine free elections, democratic institutions and values and the rule of law.

609. In late May 2019, Monica Bickert, FB's V.P. Product Policy, publicly defended FB having allowed a doctored derogatory video of House Speaker Nancy Pelosi, to run on the FB platform, stating "FB will continue to host a video of Nancy Pelosi that has been edited to give the impression that the Democratic House speaker is drunk or unwell."

610. The Pelosi defamation facilitated by FB is but the latest incident highlighting FB's willful failures to deal with disinformation, misinformation, lies and hate speech.

611. Rudy Giuliani, the President's personal lawyer, was among the President's supporters who promoted the derogatory Pelosi video He tweeted a link to a copy of the video on FB stating: "What is wrong with Nancy Pelosi? Her speech pattern is bizarre."

612. One version of the doctored Pelosi video, which FB has allowed to continue running on a FB page is entitled "Politics WatchDog" and has been viewed millions of times, attracting comments speculating on Pelosi's health, supposed use of drugs, and other apparent ailments.

613. Despite the apparently malicious intent of the video's creator, FB has said it will only downgrade its visibility in users' newsfeeds and attach a link to a third party factchecking site pointing out that the clip is misleading.

614. As a result, although it is less likely to be seen by accident, the doctored video will continue to be seen.

615. FB was forced into taking this excruciating minimalist remedial action after the *Washington Post* reported the story.

616. The President tweeted a different altered video of Pelosi, which aired on a *Fox News* business broadcast, and had been heavily edited to make it appear as if she was stuttering and slurring her language. The President's tweet said: "PELOSI STAMMERS THROUGH NEWS CONFERENCE".

617. Alarming concerns have been raised about the enormous impact of the future use of disturbingly realistic fake or doctored videos by election riggers and other miscreants.

618. In addition to suffering the tortious and possibly treasonous conduct of FB Defendants, Zimmerman had a reasonable expectation of privacy when using FB to engage in online activity; and (2) a reasonable expectation that FB would not participate with Russian operatives the Trump Campaign, Robert Mercer and others in conduct that eventually led to the successful sabotage of the 2016 U.S. presidential elections.

619. Third parties tracked and extracted Plaintiff's FB user' information from FB's information repository, tracking and extracting that Plaintiffs did not authorize and by doing so willfully intruded into Zimmerman's solitude, seclusion and private affairs.

620. FB willfully designed its platform and established policies and procedures governing its use in such a way so as to readily enable the plundering, without any authorization by Plaintiffs of Plaintiff's FB user' information and that of their FB

"Friends" by third parties.

621. Numerous privacy intrusions by third parties were and are highly offensive to Plaintiffs and would be to any reasonable person or business. This is evidenced by the immense public outcry following the revelation of FB's failure to protect the privacy of ts users' FB-stored information.

622. Further, the extent of the intrusions on Zimmerman's right to privacy and the extent to which that plundered information was used and for what purposes will never be fully known because privacy intrusions and information plunders involve obtaining and sharing Plaintiffs FB user' information and that of their FB user' with potentially known unknown third parties for unknown purposes in perpetuity.

623. During the 2016 U.S. presidential elections a majority of Americans received more fake news and fake stories than factual news and stories broadcast over FB, FB-owned Instagram and FB-owned WhatsApp.

624. Of the twenty most shared fake news and stories broadcast over FB-owned platforms during the final phase of the 2016 U.S. presidential elections seventeen were either pro-Trump or anti-Clinton. See *How to Rig and Election*, chapter 4, by Nic Cheeseman and Brian Klaas.

625. As a direct and proximate result of the conduct of FB, Plaintiffs have sustained significant harm, entitling them to nominal and punitive damages in an amount to be established at trial.

626. Inasmuch as FB have amassed massive amounts of wealth, only a massive award

of punitive damages is likely to deter FB from engaging in future election sabotage and related unconstitutional and tortious conduct.

COUNT FOUR– BREACH OF THE IMPLIED COVENENT OF GOOD FAITH AND FAIR DEALING

627. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

628. Every contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement." See *Restatement (Second) of Contracts* § 205 (1981).

629. Plaintiffs were required by FB-constructed contracts to provide their personal and business information in order to register to use the FB platform and always used it responsibly.

630. Implicit and explicit in the contractual agreements between FB and Plaintiffs was FB's obligation to protect the privacy of the Plaintiff's FB user' information.

631. Even if not explicitly stated, which it was, FB's information privacy protection duty is read into contracts and functions as a supplement to the express contractual covenants in order to prevent a transgressing party from engaging in conduct which (while not technically transgressing the express covenants) frustrates the other party's rights to the benefit of the contract.

632. Thus, any claim on the part of FB that technically it was permitted to allow the collection and transmittal of Plaintiff's FB user' information must be read in the context

of, and give way to, those user's rights to the benefit of the contract, including the terms strictly delimiting such activity.

633. The duty to perform contractual obligations in good faith applies to FB's agreements governing information collection, use, and protection, including its "Terms of Service," "Information Use Policy" and "Statement of Rights and Responsibilities."

634. In order not to frustrate the reasonable expectations of Plaintiffs under these sections and others in the FB-constructed contract and generally, FB was bound not to allow the access, collection, and transfer of Plaintiff's FB user' information to any third party.

635. But by failing to act reasonably in securing the privacy of Plaintiff's FB user' information, FB breached the covenant of good faith and fair dealing.

636. As a result of the aforesaid breach of the implied covenant of good faith and fair dealing, Plaintiffs have been harmed and have suffered damages by way of the widespread past and future dissemination of their FB user' information and that of their FB "Friends."

637. At a minimum, even if Plaintiffs had not suffered equitable or other damages nominal damages recoverable under Cal. Civ. Code § 3360.77.

COUNT FIVE-INVASION OF PRIVACY–PUBLIC DISCLOSURE OF PRIVATE FACTS

638. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

639. Plaintiffs assert this Claim under California law

640. FB is a "person" within the meaning of the California Consumer Legal Remedies ("CLRA") in that it is a corporation.

641. Plaintiffs are "consumers" within the meaning of CLRA in that they are individuals who seek or acquire services for personal, family, or business purposes.

642. CLRA § 1770(a)(5) prohibits "…representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have or that a person has a sponsorship, approval, status, affiliation, or connection which he or she does not have."

643. CLRA § 1770(a)(14) prohibits "...representing that a transaction confers or involves rights, remedies, or obligations that it does not have or involve, or that are prohibited by law."

644. . FB's conduct as alleged herein violates CLRA's ban of proscribed practices at Cal. Civ. Code ("CCC") § 1770(a) subdivisions (5) and (14) in that, among other things, FB misrepresented its services by failing to disclose that it would and did allow access to its users' information to its business partners, mobile carriers, software makers, security firms, banks, chip designers, device makers, retailers, wholesalers and numerous other third parties without FB user consent.

645. The FB user information privacy protection promises were false promises and entirely illusory.

646. With respect to "whitelisted" applications, FB collected revenue for the continued unfettered access to Plaintiffs' information and did not disclose that it was doing so, nor did FB

offer to pay Plaintiffs for the use of their information by "whitelisted" applications, or any other third party or FB itself.

647. Plaintiffs have suffered injuries caused by FB's misrepresentations and omissions because Plaintiffs suffered an invasion of their privacy as a result of FB exposing their information to its numerous third parties and were deprived of the income FB generated through its unauthorized use and sale of their information.

648. Plaintiffs seek equitable relief for FB's violations of CLRA, including injunctive relief to enjoin the wrongful practices alleged herein, and to take corrective action to remedy past conduct, including ending all information-sharing partnerships still in effect and having FB direct all device makers, business partners, and "whitelisted" applications with Plaintiffs' information stored in their information repositories to delete that information.

649. Sandberg, like Zuckerberg, has admitted FB's numerous failures to protect the privacy of FB users' information as well as Russia's use of the FB platform to sabotage the US 2016 presidential election cycle.

650. Sandberg said: "There are things that we missed. We wish we had understood the Russian interference in the US election. We didn't. We missed it."

651. Sandberg avoided answering more pressing questions over the distribution of FB users' private information.

652. Recently, an investigative reporters revealed that FB had ignored the privacy concerns of its users in a series of 2012 emails despite signing a "Consent Decree" with the FTC that mandated that FB fix their numerous failures to protect the privacy of their users' information.

653. When asked by Caroline Hyde, a business news anchor on Bloomberg TV, to address its users privacy concerns of its users, Sandberg said: "I think there has been a growing understanding of how important privacy is and how we have to protect it. " I think if you look at some of the early iterations of the FB platform, we were allowing people to share too much information early on before 2014. If I used an app, I would share my information and my friend's information. It's really hard to remember — this is not an excuse because I think we should have done better, the real concern then, was we were hoarding information and not sharing it. People were very concerned that we were a walled garden."

654. Sandberg explained that through trial and error FB realized it needed to share the "minimum amount of information."

655. Sandberg compared FB to any new technology, from the printing press to radio or TV stating that: "There is some commonality to this experience. A new technology comes out. People celebrate it to see all the good it does, almost to the exclusion of any bad, then something bad happens, and people see that the bad can happen and they focus on that. That's where the new rules are written," she said. "New rules need to be written for the Internet and we want to be part of that."

656. Later, Sandberg deflected a question on the call of FB co-founder Chris Hughes for the breaking up of FB stating: "When you think about what's underlying this conversation is that people are worried about the size and power of US tech companies whether it's ours or others. We understand that … we have a big impact in the world.,"

she said before turning to what she called a bigger threat. "People aren't appropriately worried about Chinese companies, some of which are far bigger and have far many more people and services than we do, and I think that's something that needs to be taken into account."

657. Hyde wrapped up the interview asking Sandberg if she ever questioned her role as a leader given the onslaught of company disasters.

658. "Of course. I don't know any good leaders that didn't," Sandberg said. "When we missed what happened with the Russian election, when we failed to respond quickly enough to Cambridge Analytica, of course."

COUNT SIX-CIVIL CONVERSION

659. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

660. Civil conversion is the wrongful exercise of dominion over the property of another. Here, FB Defendants exercised dominion over Plaintiff's FB user' information.

661. The elements of a claim for civil conversion are: (1) the plaintiff's ownership or right to possession of the property unlawfully converted by defendants; (2) the defendant's conversion by a wrongful act or disposition of property rights; and (3) damages." See *Lee v. Hanley* (2015) Cal.4th 1225, 1240 [191 Cal.Rptr.3d 536, 354 P.3d 334].

662. Here, the Plaintiff's right of ownership is undisputable. Here, FB Defendants have repeatedly admitted their wrongful and willful and reckless exercise of dominion over

Plaintiff's property, namely their FB user information, and disposed of it in numerous and various ways, and Plaintiffs are seeking appropriate damages.

663. It is not necessary that there be a manual taking of the property; it is only necessary to show an assumption of control or ownership over the property, or that the alleged converter has applied the property to his own use. See *Shopoff & Cavallo LLP v. Hyon* (2008) 167 Cal.App.4th 1489, 1507 [85 Cal.Rptr.3d 268].

664. Any act of dominion wrongfully exerted over the personal property of another inconsistent with the owner's rights thereto constitutes conversion. See *Plummer v. Day/Eisenberg, LLP* (2010) 184 Cal.App.4th 38, 50 [108 Cal.Rptr.3d 455].

665. Conversion is a strict liability tort. The foundation of the action rests neither in the knowledge nor the intent of the defendant. Instead, the tort consists in the breach of an absolute duty; the act of conversion itself is tortious.

666. Therefore, questions of the defendant's good faith, lack of knowledge, and motive are immaterial." See *Los Angeles Federal Credit Union v. Madatyan* (2012), 209 Cal.App.4th 1383, 1387 [147 Cal.Rptr.3d 768].

667. "The rule of strict liability applies equally to purchasers of converted goods, or more generally to purchasers from sellers who lack the power to transfer ownership of the goods sold. That is, there is no general exception for bona fide purchasers." See *Regent Alliance Ltd.,* 231 Cal.App.4th at p. 1181.

668. As the result of FB Defendants willful and reckless unlawful conversion activities, FB Defendants have willfully and recklessly interfered with Plaintiff's right of possession and control of their FB user' information.

669. As a direct and proximate result of FB's willfully unlawful conduct, Plaintiffs suffered injury, damage, loss and other harms and therefore seek compensatory damages in an amount to be established at trial.

670. As a direct and proximate result of the conduct of FB in converting Plaintiff's FB user' information, FB Defendants have acted with malice, oppression and in conscious disregard of the Plaintiff's privacy rights and Plaintiffs, therefore, seek an award of punitive damages in an amount to be established at trial.

COUNT SEVEN-NEGLIGENCE AND GROSS NEGLIGENCE

671. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

672. FBs owed a duty to Plaintiffs to exercise reasonable care in the obtaining, using, and protecting of their FB user' information, arising from the sensitivity of their information and the expectation that their information was not going to be shared with third parties without their consent.

673. This duty included FB ensuring that no application developers, device makers or other third parties were collecting, storing, obtaining and/or selling Plaintiffs' FB user' information.

674. Plaintiffs' willingness to entrust FB with their information was predicated on the

understanding that FB would take appropriate measures to protect it.

675. FB had a special relationship with Plaintiffs as a result of being entrusted with their information, which provided an independent special duty of care.

676. FB knew that the information of Plaintiffs had value because there is an active market for FB user' information. Indeed, FB has received tens of billions of dollars from selling targeted advertising on its platform.

677. There is also an active black market for FB user' information.

678. FB received multiple warnings that its user' information was at risk.

679. In 2012, Sandy Parakilas, former FB operations manager warned FB's executives about the risks of application developers gaining unfettered access to FB information without their consent.

680. According to Parakilas, FB was not conducting regular audits of application developers use of the FB's platform.

681. FB ignored Parakilas's warning.

682. In 2012, FB executed a "Consent Decree" with the FTC agreeing to, among other things, clearly and prominently disclose its sharing of FB user' information with third parties.

683. Even so, FB continued to let application developers access its users' information without their consent.

684. And, as late as 2017, Alex Stamos, FB's then Chief of Security, warned FB executives about security risks on the platform in a written report concerning the circumstances leading to Cambridge Analytica obtaining FB users'

personal information.

685. Despite these and other numerous warnings, FB failed to take reasonable steps to prevent harm to Plaintiffs and its other users.

686. On April 30, 2014, FB announced a new "anonymous login" feature that would have allowed users to use an application without sharing any personal information. Yet, FB never implemented this feature.

687. On April 30, 2104, FB also announced a new "controlled login" feature to allow users to choose what information they shared with application developers before login in, but FB did not implement this feature until May 2015.

688. As early as December 11, 2015, FB received notice that application developer Aleksandr Kogan had sold FB user' personal information to Cambridge Analytica; but FB waited until April 2018, more than three years later, to notify users that their personal information had been unlawfully misappropriated.

689. FB owed a duty to timely disclose to Plaintiffs that FB had allowed their information to be accessed by Cambridge Analytica and numerous other third parties.

690. Plaintiffs had a reasonable expectation that FB would information them of the improper disclosure of their information.

691. FB breached its duties by, among other things: (a) failing to ensure that application developers, "whitelisted" applications, device makers and other third parties were not improperly collecting, storing, obtaining and/or selling Plaintiffs' information without their informed consent; and (b) failing to provide adequate and timely notice that Plaintiff's FB-stored content and information had been improperly obtained by Cambridge Analytica and

numerous third parties.

692. But for FB's breach of its duties, including its duty to use reasonable care to protect and secure Plaintiff's information, Plaintiff's information would not have been disclosed without their consent to third parties, which resulted in further misuse of Plaintiff's information.

693. Plaintiffs were foreseeable victims of FB's breach of its duties.

694. FB knew or should have known that allowing third parties to access Plaintiff's ' information would cause damage to Plaintiffs.

695. Public policy voids any waiver of liability that FB Defendants may raise.

696. The contracts between FB and Plaintiffs are of a type suitable for public regulation.

697. Indeed, FB is subject to public regulation due to its ubiquity and use by over a hundred million of Americans.

698. Using FB is often a matter of practical necessity for the many persons and businesses who are now addicted to use FB to coordinate daily activities, network, engage in political and cultural discourse and pursue interests and hobbies. To do these things, FB users must share their personal information with their FB "Friends."

699. FB maintains it is a free provider of communication services that wants to connect every person on planet Earth

700. Because of its enormous financial resources and monopolistic power, FB possesses a decisive advantage when dealing with any member of the public that seeks to use its

services, making any purported waiver of liability by FB unconscionable and unlawful.

701. The confidentiality of Plaintiff's FB user' information was and still is totally under FB's control.

702. FB violated its very own privacy protection promises by allowing numerous third parties to access Plaintiff's user' information.

703. Beyond mere negligence, FB's conduct also constitutes gross negligence due to FB's willful and reckless departure from ordinary standards of care and its knowledge that it had failed to secure the information of Plaintiffs and did nothing about it, including failing to notify Plaintiffs of its information privacy protection failures and doing nothing to correct those failures and even denying that the failures occurred.

704. As a result of FB's failure to safeguard Plaintiffs' user' information, Plaintiffs have suffered injury, which includes but is not limited to impermissible disclosure of their information, both directly and indirectly by FB, and exposure to a heightened, imminent risk of misuse, fraud, identity theft, voter fraud, medical fraud, and financial and other harms.

705. The information shared by FB with third parties allows this information to be aggregated with other information and allows third parties to identify and target Plaintiffs.

706. The injury to Plaintiffs was a proximate and reasonably foreseeable result of FB's breaches of its contractual duties and promises to Plaintiffs.

707. As a proximate result of FB's information privacy protection failures, Plaintiffs suffered damages in an amount to be established at trial.

COUNT EIGHT-NEGLIGENT AND/OR FRAUDULENT MISREPRESENTATION

708. Plaintiffs incorporate by reference all paragraphs of this Complaint as though fully set forth herein.

709. Plaintiffs suffered injury in fact and lost money or property as the proximate result of FB's negligent and/or fraudulent misrepresentations.

710. The FB user' information of Plaintiffs was taken by third parties who will and did use it for their own advantage.

711. Plaintiffs justifiably relied on the representations FB made in its publicly available privacy policy and elsewhere that it would not "share information we receive about you with others unless we have: received your permission [and] given you notice."

712. FB knew the falsity of its privacy protection representations, and they were made with the intent to deceive Plaintiffs into supplying FB with private confidential personal information.

713. FB's representations regarding the maintenance of user confidentiality and privacy were material to Plaintiffs' decision to provide FB with the personal information FB subsequently disclosed to numerous third parties.

714. Plaintiffs justifiably relied upon the representations of FB.

715. Plaintiffs suffered harm as a proximate result of FB's fraudulent acts.

716. As a direct and indirect result of FB's negligent and/or fraudulent misrepresentations, Plaintiffs are entitled to general, special punitive damages, reasonable

attorneys' fees if any, and costs, and any other relief in an amount to be established at trial.

COUNT NINE BREACH OF CONTRACT

717. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

718. At all relevant times, FB and Plaintiffs mutually assented to, and were bound by the version of FB's "Statement of Rights and Responsibilities" or later, the "Terms of Service," that was operative at the time each of the Plaintiffs registered to use the FB platform.

719. At all relevant times, FB affirmed that FB would "not share your information with advertisers without your consent." None of FB contracts informed and obtained users' meaningful and lawfully obtained consent to share their information with advertisers and other third parties, or disclosed that such information would be shared if FB users' "Friends" entered into an agreement which permitted third parties to collect their FB "Friends'" information.

720. Thus, the FB non-negotiable, non-negotiable contracts did not authorize FB to share Plaintiffs' user' information with FB's business partners or mobile carriers, software makers, security firms, banks, credit reporting and government agencies, chip designers, device makers, retailers, wholesalers or any other third party.

721. The FB contracts with Plaintiffs also did not authorize FB to make the information that users shared with "Friends" available to any third party.

722. Contrary to the FB contracts with Plaintiffs, FB knowingly allowed numerous third parties who made their applications available through Graph API v1.0 to sell the information regarding Plaintiffs that they had collected via applications that used the FB platform.

723. The FB contracts required FB to protect the information of its users.

724. The FB contracts affirm that users' information would not be shared with advertisers or any other third party without their affirmative consent.

725. Likewise, these same FB "Terms of Service" informed users that their privacy setting would control who had access to their content and information, but this was untrue. FB did not disclose that users were required to affirmatively "opt out" of sharing their information with third parties in the FB contracts.

726. As set forth herein, Plaintiffs' information is of considerable value as demonstrated by FB's calculation of the Average Revenue Per User that FB calculates.

727. There is an active market for the information generated by FB users, both individually and especially in the aggregate. FB generates billions of dollars in revenues through targeted advertising delivered to third parties, curated through the collection and aggregation of FB's user information.

728. There is also an active black market for user information.

729. The remedy for the FB breaches of the FB contracts is what FB gained through their breaches.

730. The value of the information accumulated by FB about a user increases with the amount of information FB collects. Thus, over time, FB's benefit of the bargain has multiplied dramatically.

731. . As a result of the breach, Plaintiffs have been harmed and have suffered damages by losing the value of their information.

COUNT TEN-WILLFUL INFLICTION OF EMOTIONAL DISTRESS

732. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

733. FB knew and were plainly indifferent to the fact that their blocking of Plaintiff's FB personal and business accounts would cause Zimmerman severe emotional distress.

734. FB knew that their failure to protect Plaintiff's user' information from access by third parties not authorized for such access by him would cause Zimmerman severe emotional distress.

735. FB knew that Plaintiff's plundered FB user' information was not intended for use in sabotaging the 2016 U.S. presidential elections or other U.S. elections and such use would cause Zimmerman severe emotional distress.

736. The willful unlawful conduct of FB as set out in this Complaint was extreme, outrageous, and beyond the bounds of decency.

737. As a direct and proximate result of the conduct of FB, Zimmerman has suffered severe or extreme emotional distress, entitling him to recover damages in an amount to be established at trial.

738. The outrageous, malicious, and willful misconduct of FB conspiring with a hostile foreign governments and others to use Plaintiff's plundered FB user' information to influence the2016 U.S. presidential elections and other purposes entitles Plaintiffs to receive punitive damages so as to deter FB from repeating such outrageous conduct in the future.

COUNT ELEVEN-COMMON LAW CIVIL CONSPIRACY

739. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

740. "The basis of a civil conspiracy is the formation of a group of two or more persons who have agreed to a common plan or design to commit a tortious act.' The conspiring FBs must also have actual knowledge that a tort is planned and concur in the tortious scheme with knowledge of its unlawful purpose." See *Kidron v. Movie Acquisition Corp.*, 40 Cal.App.4th 1571, 1582 (1995). A conspiracy may be inferred from circumstances, including the nature of the acts done, the relationships between the parties, and the interests of the alleged co-conspirators.

741. Well before information repositories, FB knew and have admitted that they knew that FB was deliberately and for its own profit and other purposes allowing third parties to access and collect Plaintiff's user' information without his consent and that FB's

information security measures were so grossly inadequate that malevolent third parties could also access and collect Plaintiff's user' information. Nevertheless, FB continued to recklessly ignore FB's gigantic information security problem and instead did little to nothing to protect Plaintiff's FB user' information or even bother to warn them about the security problems and, instead, openly lied to Congress and foreign governments that FB was dedicated to the highest and most advance security practices and protocols.

742. FB willfully opted to not disclose to Plaintiffs that their FB accounts and associated user information are an easy target for information plunderers and that FB was not implementing measures to protect them.

743. FB conspired among themselves and with others, including the Trump Campaign, Robert Mercer and Russian officials, agents and operatives to act in concert for unlawful purposes by unlawful means as described in detail throughout this Complaint and have admitted as much. See Section X and the entirety contained throughout this Complaint.

744. In particular, FB and their co-conspirators agreed to publicly disclose on the Internet and elsewhere Plaintiff's FB user' information and that of their FB "Friends" that were plundered from FB by Cambridge Analytica, a now bankrupt business entity funded, directed and controlled by Mercer and deliberately allowed third parties to access and collect Plaintiff's FB user' information without Plaintiff's consent or knowledge.

745. FB conspiratorial conduct violated California civil conspiracy law that maintains that a conspiracy is an agreement by two or more persons, Mark Zuckerberg, Sheryl Sandberg and other FB executives to commit a wrongful act.

746. Such an agreement may be made orally or in writing or may be implied by the conduct of the parties. A conspiracy may be inferred from circumstances, including the nature of the acts done, the relationships between the parties, and the interests of the alleged co-conspirators. "While criminal conspiracies involve distinct substantive wrongs, civil conspiracies do not involve separate torts. The doctrine provides a remedial measure for affixing liability to all persons who have 'agreed to a common design to commit a wrong.'" See *Choate v. County of Orange* (2000) 86. Cal.App.4th 312, 333 [103 Cal.Rptr.2d 339].

747. "As long as two or more persons agree to perform a wrongful act, the law places civil liability for the resulting damages on all of them, regardless of whether they actually commit the tort themselves. 'The effect of charging . . .conspiratorial conduct is to implicate all . . . who agree to the plan to commit the wrong as well as those who actually carry it out.' " See *Wyatt v. Union Mortgage Co.* (1979) 24 Cal.3d 773, 784 [157 Cal. Rptr. 392, 598 P.2d 45].

748. "Conspiracy is not a cause of action, but a legal doctrine that imposes liability on persons who, although not actually committing a tort themselves, share with the immediate tortfeasors a common plan or design in its perpetration.

749. By participation in a civil conspiracy, a co-conspirator effectively adopts as his or her own the torts of other co-conspirators within the ambit of the conspiracy. In this way, a co-conspirator incurs tort liability co-equal with the immediate tortfeasors." See *Applied Equipment Corp. v. Litton Saudi Arabia Ltd.* (1994) 7 Cal.4th 503, 510–511 [28 Cal.Rptr.2d 475, 869 P.2d 454]

750. As a direct and proximate result of the overt and covert acts of FB, Plaintiffs have sustained significant harm, entitling them to recover damages in an amount to established at trial.

COUNT TWELVE-DECEIT BY CONCEALMENT OR OMISSION

751. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

752. Under California law, a plaintiff may assert a claim for deceit by concealment based on "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact." CCC § 1710(3).

753. These following actions are "deceit" under CCC § 1710 because FB suppressed facts that they were duty-bound to disclose, especially given FB's assertions about protecting the privacy of Plaintiffs. FB has committed deceit by concealment in three distinct ways.

754. FB did not disclose known risks that third party application developers would sell or disperse user information. FB received multiple warnings that Plaintiffs' information was at risk.

755. In 2012, Sandy Parakilas, former FB operations manager, warned FB's executives about the risks of application developers gaining unfettered access to users' personal information without their consent on FB's platform. Yet, FB ignored Parakilas's warnings.

756. In October 2012, FB reached a settlement with the FTC agreeing to clearly and prominently disclose its sharing of information with third parties; yet, FB continued to let application developers access users' information without their consent.

757. As late as 2017, Alex Stamos, FB's former Chief of Security, warned FB executives about security risks on the platform. In an internal meeting held in 2017, Stamos warned of "willful decisions to give unfettered access to information and systems to engineers to make them 'move fast' but that creates other issues for us."

758. In 2017, Stamos states that he provided a written report concerning the circumstances leading to Cambridge Analytica obtaining users' personal information. FB edited and published a whitewashed version of this report concealing any wrongdoing.

759. FB did not audit what happened to information that was provided to third parties because it knew it would find abuse. FB did not disclose to Plaintiffs the risks that they faced from these warnings and did not inform Plaintiffs that their information was insecure once it was shared with application developers or other third parties.

760. FB knew that Plaintiffs' information was not secure. Even so, FB ignored the warnings above that audits were necessary to secure Plaintiffs' information because FBs did not know what third parties were doing with it after it left FB's servers.

761. FB willfully, deceptively and recklessly failed to secure Plaintiffs' FB user' information and content because they wanted to encourage application developers, FB business partners and numerous other third parties to exploit that information and content. FBs knew that appropriate security measures, such as audits, would discourage third

parties. FBs did not engage in such audits or conduct other reasonable efforts to protect Plaintiffs' information.

762. FB had a duty to inform Plaintiffs that FB had become aware that they had failed to secure their information. FB knew in 2015 that it had failed to secure Plaintiffs' information, including by making it available to numerous third parties.

763. FB willfully concealed that Plaintiffs' FB user information and content was insecure because they wanted Plaintiffs to continue to generate content for their business partners.

764. FB failed to disclose the risks Plaintiffs faced with the intention to deceive them about the security of their information.

765. FB failed to disclose to Plaintiffs that it had failed to secure information for dozens of other third party Applications, even after they became aware of the Cambridge Analytica unlawful misappropriation of FB user' information from tens-of-millions of FB users and failed to conduct any investigation into the extent or use of the FB user' information to which it until March of 2018.

766. Plaintiffs been aware that FB had failed to implement adequate security measures, they would not have shared their information and content with FB to the extent that they did, if at all.

767. Plaintiffs were damaged because, as a result of FBs' deceit, their content and information have been disclosed to third parties without their consent.

768. Plaintiffs were also damaged because, as a result of FBs' deceit, their privacy was invaded.

769. Plaintiffs are at heightened risk of identity theft, phishing schemes, and other malicious attacks. Due to FB's deceit, Plaintiffs' information and content were compromised, and may be available on the dark web or in the hands of foreign nationals.

770. Plaintiffs are therefore entitled to "any damage" that they have suffered under CCC Section 1709.

771. FB have also committed deceit by failing to meaningfully disclose to Plaintiffs how FB allows other third parties, including but not limited to application developers, "whitelisted" applications, device makers, mobile carriers, software makers, and others to obtain their FB user' information notwithstanding their privacy settings.

772. With respect to "whitelisted" applications, FB failed to disclose that FB would provide the applications with FB users' information as long as the "whitelisted" applications provided FB with revenues that were based on how many FB users' information they accessed.

773. FB failed to disclose that these FB users and their "Friends" could not control "whitelisted" applications' access with their privacy settings.

774. FB allowed "whitelisted" applications to continue to receive information from users and their "Friends" notwithstanding users' privacy settings.

775. FB stripped privacy settings from photos and videos that had been designated private, in violation of its own privacy policies. As a result, those applications could not honor users' privacy settings.

776. In addition, computer applications were able to circumvent FB user's privacy of platform settings and access FB "Friend's" information, even when the FB user disabled the FB Platform.

777. FB misled users to believe that they were protecting users' privacy and failed to disclose that they were sharing users' information with third parties.

778. FB did not disclose that, notwithstanding privacy settings that purported toprovide Plaintiffs with control over their information, FB allowed third -parties to harvest and store personal information.

779. FB had a duty to provide accurate information to Plaintiffs about how their information was disclosed to third parties by FB. FBs knew that Plaintiffs shared personal and sometimes intimate details about their lives, personalities, and identities.

780. FB encouraged Plaintiffs to share information by assuring them that FB would respect their choices concerning privacy.

781. FB willfully concealed and omitted material information regarding how FB disclosed Plaintiffs' information in an effort to create a false sense of security and privacy for Plaintiffs.

782. FB did this because they wanted Plaintiffs to provide more detailed information, whose value would be increased by that additional detail. Third parties would thereby pay a higher price for unfettered access to that information, increasing FB's revenue.

783. Had Plaintiffs been aware of the full extent of how FB collected and used their information, they would not have shared their information on their devices on the FB platform to the same degree that they did, if at all.

784. Plaintiffs were damaged because their information was disclosed to third party device makers and others without their consent.

785. As a result of the disclosures of Plaintiffs' FB user' information to these third parties, Plaintiffs could not take remedial measures to protect themselves from identity theft, scams, phishing, unwanted political targeting, even surveillance and other forms of harassment.

786. Moreover, Plaintiffs would have behaved differently and shared less information had these acts been disclosed.

787. FB deliberately withheld notice because it did not want to discourage user sharing and engagement on its platform.

788. FB also failed to disclose to Plaintiffs how their Fb user' information was being collected, shared and aggregated to develop digital profiles or dossiers of each FB user.

789. Those dossiers comprised of FB user information were combined with other sources to de-anonymize this information such that FB users could be individual targeted.

790. FB had a duty to disclose the full extent to which it allowed Plaintiffs to be targeted by advertisers and marketers because it promised in its Contracts that it would not share users' information with advertisers without their consent. FBs' duty also arose from its affirmative representations that (1) Plaintiffs could control their information, and (2) third parties could not access personal information absent users' consent.

791. FB knew that advertisers were targeting Plaintiffs with messages based upon FB derived information, combined with information derived from other information brokers.

792. FB was the vehicle to target Plaintiffs by drawing upon the vast amounts of content information collected by FB and matched with additional information collected about them by third party information brokers.

793. FB knew that psychographic marketing and other targeted advertising was lucrative, and that advertisers paid a premium to combine FB user' information with information from third party information brokers.

794. FB did not disclose to Plaintiffs that advertisers were combining information from information brokers with FB-derived information to target them with advertisements and psychographic marketing, as well as building digital dossiers.

795. FB intended to deceive Plaintiffs about their vulnerability to targeted advertisements and about the degree to which sharing their FB user' information and content on FB directly led to targeted messaging.

796. Had Plaintiffs known the extent to which FB shared their information with third parties, and how it was aggregated and made available to advertisers and political operatives and others, Plaintiffs would have not shared their information and content on FB to the extent that they did, if it all.

797. Plaintiffs suffered injury as a direct result of FB' deceit.

798. Plaintiffs FB user' information and content were used and aggregated by advertisers and other third parties without their consent, and for nefarious purposes and in return FB received substantial advertising revenues.

799. Had Plaintiffs known the extent and degree to which their FB user' information was provided to third parties Plaintiffs would have required compensation for this use of their FB user information.

800. Plaintiffs suffered economic injury as a result of FB's fraud. Plaintiffs have an economic and privacy interest in their FB user' information, which has value beyond the FB platform.

801. FB knew that Plaintiff's FB user' information was worth at least $0.10 for each application to view a FB user's profile, and FB orchestrated its "whitelisting" to require applications to pay to FB revenues that were equivalent to the number of Fb users and their "Friends" that each application had.

802. As a result, FB have been unjustly enriched by its deceit, and Plaintiffs are entitled to restitution.

803. Restitution is a remedy that may be awarded to prevent unjust enrichment when the FB has obtained some benefit from Plaintiffs through fraud, duress, conversion or similar misconduct. See *McBride v. Boughton,* 123 Cal.App.4th 379, 387–388 (2004).

804. For all types of fraudulent omissions complained of here, Plaintiffs s seek disgorgement of FB's profits that were made with the use of Plaintiff's FB user' information.

805. Disgorgement is appropriate because FB profited from Plaintiffs' content and information wrongfully obtained by generating revenues from third party computer application developers and advertisers.

806. Disgorgement is necessary in order to deter future unauthorized use of Plaintiff's FB user' information. Disgorgement is also necessary to the extent that the value of Plaintiff's user' information cannot be assessed by ordinary tort damages. Public policy supports the use of disgorgement here to disincentivize the type of deception that FB used in exploiting Plaintiff's FB user information.

807. In the future, as a direct result of FB's unlawful conduct Plaintiffs may also suffer further damages of a nature that are purely speculative at this time.

808. Accordingly, as a result of the misconduct of FB, Plaintiffs are entitled to recover damages, including punitive damages under CCC § 3294(a) in an amount to be established at trial.

COUNT THIRTEEN-FRAUD

809. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

810. FB deceit as alleged herein is fraud under CCC § 3294(c)(3) in that it was deceit or concealment of a material fact known to the FB and FB willfully deprived Plaintiffs of legal rights and otherwise caused injury to them.

811. "The elements of fraud that will give rise to a tort action for deceit are: "(a)

misrepresentation (false representation, concealment, or nondisclosure); (b) knowledge of falsity (or 'scienter'); (c) intent to defraud, i.e., to induce reliance; (d) justifiable reliance; and (e) resulting damage.' " See *Engalla v. Permanente Medical Group, Inc.* (1997) 15 Cal.4th 951, 974 [64 Cal.Rptr.2d 843, 938 P.2d 903]; *Medallion, Inc. v. Clorox Co.* (1996) 44 Cal.App.4th 1807, 1816 [52 Cal.Rptr.2d 650] [combining misrepresentation and scienter as a single element].

812. "Fraud is a willful tort; it is the element of fraudulent intent, or intent to deceive, that distinguishes it from actionable negligent misrepresentation and from nonactionable innocent misrepresentation.

813. It is the element of intent which makes fraud actionable, irrespective of any contractual or fiduciary duty one party might owe to the other." See *City of Atascadero v. Merrill Lynch, Pierce, Fenner & Smith* (1998) 68 Cal.App.4th 445, 482 [80 Cal.Rptr.2d 329]. Fraudulent intent is an issue for the trier of fact to decide." See *Beckwith v. Dahl,* (2012) 205 Cal.App.4th 1039, 1061.

814. As a direct and proximate result of the overt and covert acts of FB as alleged throughout this Complaint, Plaintiffs have sustained significant harm, entitling them to recover damages in an amount to established at trial.

COUNT FOURTEEN- WILLFUL MISREPRESENTATION

815. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

816. Plaintiffs claim that FB willfully and for profit and other purposes made at least one important false representation that substantially harmed Plaintiffs, that being that they would protect the privacy of Plaintiff's FB user' information.

817. When the FB made that false representation, they knew it was false and misleading and made it with a conscious and reckless disregard for the truth.

818. FB intended that Plaintiffs rely on their misrepresentation.

819. Zimmerman did reasonably rely on FB's misrepresentation.

820. Plaintiffs were harmed and Plaintiff Zimmerman's reliance on FB's representation was a substantial factor in causing that harm.

821. These willful misrepresentations by FB constitute "deceit" under CCC § 1710 in that it is suppression of a fact by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact.

822. As a result of this deceitful misrepresentation by FB the user' information of Plaintiffs was compromised, placing Plaintiffs at a great risk of identity theft and other crimes.

823. As a result of FB's deceitful misrepresentations, FB Defendants are liable under CCC § 1709 for the damage their conduct inflicted on Plaintiffs.

824. Plaintiffs also suffered diminution in value of their information in that it may now or in the future be readily available to plunderers on the "Dark Web" and elsewhere.

825. Plaintiffs may also suffer consequential out of pocket losses for procuring credit freeze or protection services.

826. As a result of the conduct of FB Defendants, Plaintiffs are entitled to recover damages, including punitive damages under CCC § 3294(a) in an amount to be established at trial.

COUNT FIFTEEN-CIVIL RICO CONSPIRACY

827. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

828. Plaintiffs assert FB Defendants' violations of 18 U.S.C. § 1962(C) and the Enterprise constitutes a RICO Enterprise pursuant to 18 U.S.C. § 1961(4).

829. The RICO Enterprise and/or the RICO Association-in-Fact Enterprise ("Enterprise") has been operating since at least 2014 and at various times was and for the most part still is composed of FB Defendants, Russian officials, intelligence agents and operatives, the Trump Campaign, Aleksandr Kogan, Robert Mercer, Jared Kushner, Cambridge Analytica, Stephen Bannon and numerous other persons and entities.

830. The Enterprise engaged in, and still engages in, activities that affect interstate commerce.

831. The Enterprise was formed for the purpose of using unlawfully obtained FB user' information and other unlawfully obtained information for the targeted transmission to prospective voters of political propaganda, misinformation, disinformation, misleading political advertising and other messaging.to, as matters turned out, successfully help sabotage the 2016 U.S. election cycle.

832. Aleksandr Kogan participated in the Enterprise by (i) creating a U.K. company that was part of a scheme to dupe FB users' into providing their FB user' information to

to the U.K. company, which was part of a broader scheme to unlawfully plunder the FB user' information of tens-of-millions of FB users.

833. Bannon participated in the Enterprise by, among other things: (i) helping to found Cambridge Analytica by obtaining funding for Cambridge Analytica from Robert Mercer (a U.S. citizen); (ii) acting as a vice-president of Cambridge Analytica; (iii) helping to supervise the activities of Cambridge Analytica; and (iv) serving as a senior political advisor to the Trump Campaign and the Trump administration.

834. These actions were undertaken with fraud, malice and a willful conscious disregard of the rights or safety of Plaintiffs and the majority of Americans who voted in the 2016 presidential election cycle. .

835. FB Defendants agreed to and did conduct and participate, directly and indirectly, in the conduct of the Enterprise's affairs in a pattern of racketeering activity.

836. Prior to and concurrent with its participation in the Enterprise, FB willfully and recklessly devised a scheme with artifice to defraud FB users and to obtain, sell, trade and use FB user's information by false pretenses and representations, including, but not limited to, the representation that the information would only be used for academic purposes.

837. The payments made to takers of the "This is Your Digital Life" quiz were in furtherance of the fraudulent scheme and were made by wire transfer or other electronic means through interstate or foreign commerce.

838. The acts of wire fraud averred herein also constitute a pattern of racketeering activity pursuant to 18 U.S.C. § 1961(5).

839. FB aided and abetted the co-conspirators by misleading its users to believe that their FB us' information was safe, while allowing numerous third parties to access and use the information of non-consenting FB users without their permission and knowledge.

840. FB directly participated in the conspiracy by misleading quiz-takers that they were allowing third parties unfettered access to only their information for academic purposes only, when in fact they were allowing unfettered access to their FB "Friends'" information, and by fraudulently obtaining the information, selling it and trading it in interstate and foreign commerce, and using it to sabotage elections.

841. Plaintiffs were harmed by FB conduct because the private information they did not intend to become public or disclose to third parties was acquired by persons and entities who used it to unlawfully sabotage elections and other nefarious purposes.

842. Furthermore, the security breach put Plaintiffs are in imminent and real danger of having their identities stolen by anyone willing to pay these unscrupulous companies for their FB user' information.

843. In addition, Plaintiffs spent considerable time and money unsuccessfully attempting protect against the misuse of their plundered FB user information.

844. As a direct and proximate FB Defendants racketeering activities and violations of 18 U.S.C. § 1962(c), Plaintiffs have been injured and request judgment in their favor and against FB Defendants for compensatory, treble and/or punitive damages with interest,

the costs of suit and attorneys' fees, if any, , and other and further relief as this Court deems just and proper.

COUNT SIXTEEN-VIOLATION OF THE STORED COMMUNICATIONS ACT

845. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

846. The Stored Communications Act ("SCA") allows a private right of action against anyone who "(1) willfully accesses without authorization a facility through which an electronic communication service is provided; or (2) willfully exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized unfettered access to a wire or electronic communication while it is in electronic storage in such system." See 18 U.S.C. § 2701(a); see also 18 U.S.C. § 2707(a).

847. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). The SCA incorporates this definition of "electronic communication."

848. To create the information transferred to FB such as all posts, private messages, and similar communication (collectively "FB user' information" or "content"), FB users transmit writing, images, or other data via the Internet from their computers or mobile devices to FB's servers. This FB content, therefore, constitutes electronic communications for purposes of the SCA.

849. The SCA distinguishes between two types of electronic storage. The first is defined as any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). The second type is defined as "any

storage of such communication by an electronic communication for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B).

850. FB saves and stores FB user information indefinitely in electronic storage repositories.

851. Plaintiffs did not authorize FB to share their user information with any third party.

852. Pursuant to 18 U.S.C. § 2702(a)(2), before their FB accounts were blocked by FB, Plaintiffs were users of FB's remote computing service.

853. By definition, because FB provides the ability to send or receive wire or electronic communications, FB is an electronic communication service within the meaning of the SCA.

854. Pursuant to 18 U.S.C. § 2510(13,)before their FB accounts were blocked by FB, Plaintiffs were users of FB's electronic communication service.

855. Pursuant to 18 U.S.C. §§ 2707(a) and 2510(11), Plaintiffs were FB registered users who were harmed by FB's violations of the SCA.

856. Because it provides computer storage and processing services by means of an electronic communications system, FB is a remote computer service within the meaning of the SCA.

857. Pursuant to 18 U.S.C. §§ 2702(a)(1) and 2510(15), FB is a provider of an electronic communication service to the public.

.

858. Pursuant to 18 U.S.C. § 2701(a), FB maintains facilities through which an electronic communication service is provided.

859. Pursuant to 18 U.S.C. §§ 2702(a)(2) and 2711(2)FB is a provider of a remote computing service to the public.

860. Pursuant to 18 U.S.C. § 2510(6) and 18 U.S.C. § 2707(a)FB Defendants are persons or entities within the meaning of the SCA.

861. Pursuant to 18 U.S.C. §§ 2501(12), Plaintiffs use of FB's messaging systems and transfers of information to FB constitute electronic communications.

862. Pursuant to 18 U.S.C. 2501(17), Plaintiffs' electronic communications were in electronic storage repositories.

863. Pursuant to 18 U.S.C. § §2701(a) and 2702(a)(1), FBs violated the SCA by allowing access to third parties to FB's information repository that stored FB user' information and electronic communications, including Plaintiff's, and by knowingly divulging the contents, including Plaintiffs', electronic communications to numerous FB authorized third parties and unauthorized third parties.

864. Pursuant to 18 U.S.C. § 2702(a)(2),.FB also violated the SCA by knowingly divulging the contents of Plaintiffs' electronic communications that were carried or maintained on FB's remote computing service to numerous unauthorized third parties.

865. The contents of Plaintiffs' electronic communications that FB divulged to unauthorized parties were non-public, and Plaintiffs reasonably believed that the contents of these communications would be protected against publication to unauthorized parties.

866. The subsequent disclosure of FB user information by applications and business partners to additional unauthorized third parties was reasonably foreseeable, and FB knew or should have known about this subsequent disclosure.

867. FB also failed to effectively audit, limit, or control computer applications or business partners or numerous other third parties from accessing FB user' information so as to prevent the subsequent disclosure of that FB user information.

868. FB directly profited from the disclosure of FB user' information, through advertisements placed by unauthorized parties that received FB user information from applications or business partners, or numerous other third parties including Cambridge Analytica.

869. FB users of computer applications, such as "This Is Your Digital Life," were not aware of and did not consent to the disclosure of the contents of their electronic communications and their FB user' information and that of their "Friends" to unauthorized parties, including Cambridge Analytica, FB business partners, advertisers, and information brokers.

870. As a result of FBs' violations of the SCA, Plaintiffs have suffered injury, including but not limited to the invasion of Plaintiffs' privacy rights.

871. Pursuant to 18 U.S.C. § 2707(c), FB Defendants profited through their violations of the SCA, and Plaintiffs suffered actual damages as a result of these violations.

872. Plaintiffs are also entitled to preliminary and other equitable or declaratory relief as may be appropriate, as well as reasonable attorneys' fees, if any, and litigation costs pursuant to18 U.S.C. § 2707(b).

873. FB's violations of the SCA were committed deceptively, willfully and recklessly and with malice.

874. Accordingly, Plaintiffs also seek punitive damages pursuant to 18 U.S.C. § 2707(c).

COUNT SEVENTEEN-VIOLATION OF CALIFORNIA'S COMPUTER DATA ACCESS AND FRAUD ACT

875. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

876. FB knowingly accessed and without permission used Plaintiffs' content and information in order to wrongfully control or obtain property or information in violation of CPC § 502(c)(1).

877. FB' knowingly accessed and without permission took, copied, and/or used information from Plaintiffs' computers, computer systems and/or computer network in violation of CPC § 502(c)(2).

878. FB' knowingly and without permission used or caused to be used Plaintiffs' computer services in violation of CPC § 502(c)(3).

879. FB' knowingly and without permission accessed or caused to be accessed Plaintiffs' computers, computer systems, and/or computer network in violation of CPC § 502(c)(7).

880. Plaintiffs suffered and continue to suffer damage as a result of FB's violations of CPC § 502.

881. FB' conduct also caused irreparable and incalculable harm and injuries to Plaintiffs in the form of invading their privacy, and, unless enjoined, will cause further irreparable and incalculable injury, for which Plaintiffs have no adequate remedy at law.

882. FB' willfully violated CPC § 502 in disregard and derogation of the rights of Plaintiffs, and FB's actions as alleged above were carried out with oppression, fraud and malice.

883. Pursuant to CPC § 502(e), Plaintiffs are entitled to injunctive relief,

compensatory damages, punitive or exemplary damages, attorneys' fees, costs and other equitable relief.

COUNT EIGHTEEN-VIOLATIONS OF THE CALIFORNIA UNFAIR COMPTITION LAW

884. Plaintiffs incorporate by reference all paragraphs contained throughout this Complaint as though fully set forth herein.

885. The conduct of FB Defendants as alleged herein constitutes unfair, unlawful and fraudulent business acts and practices as proscribed by California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200.

886. FB violated Plaintiffs' privacy by allowing their FB user' information to be exploited in ways that Plaintiffs could not have been foreseen.

887. Plaintiffs interests were also violated by FB Defendants numerous deceptions.

888. Had Plaintiffs known the extent to which FB allowed their personal content to be collected, aggregated, pooled, and transferred for commercial purposes to companies such as Cambridge Analytica and numerous other third parties, Plaintiffs would not have placed their information on FB to the same extent they did, if at all.

889. FB allowed third party application developers, FB business partners, device makers and numerous other third parties to harvest Plaintiff's FB users' content and information and that of their FB "Friends" on a mammoth scale with zero notice to Plaintiffs.

890. FB had a duty to disclose the nature and extent of the harvesting of their FB user' information by third parties.

891. FB's conduct was and is unfair.

892. California has a strong public policy intended to protect Plaintiff's information privacy interests.

893. FB violated California's public policy by exploiting Plaintiffs' information without Plaintiff's informed consent.

894. FB's conduct also violated the interests protected by the Video Privacy Protection Act, 18 U.S.C. § 2710; the Stored Communications Act, 18 U.S.C. § 2701 et seq.; Cal. Civ. Code §§ 1709, 1710 and Article 1, § 1 of the California Constitution.

895. To establish liability under the unfair prong, Plaintiffs need not establish that these statutes were actually violated, although the claims pleaded herein do that.

896. FB never informed Plaintiffs of the uses of their FB user' information by FB and invaded Plaintiffs' privacy by subjecting their information to largescale third party access and plundering without Plaintiff's knowledge or meaningful consent.

897. FB's unlawful conduct included stripping Plaintiffs' privacy metainformation from their photos and videos and allowing numerous third parties to access and plunder Plaintiff's FB user information.

898. Plaintiffs could not have anticipated FB's intrusion into their privacy.

899. FB' conduct did not create a benefit that outweighs these strong public policy interests. FB's conduct benefitted FB and its business partners and numerous other third parties at the expense of the privacy of hundreds-of- millions of FB users, including Plaintiffs.

900. Additionally, the effects of FB's conduct were comparable to or substantially the same as the conduct forbidden by the California Constitution and the common law's

prohibitions against invasion of privacy, in that FB's conduct invaded fundamental privacy interests.

901. FB's conduct violated the spirit and letter of the several laws that protect privacy interests and prohibit misleading and deceptive practices.

902. The FB user' information that FB allowed third parties to access and plunder exposed Plaintiffs to an increased risk of identity theft, voter fraud, tax return fraud and allowed third parties to link their identities to other information in order to de-anonymize them.

903. FB's conduct is fraudulent. FB intentionally and deceptively misled Plaintiffs concerning the use of their FB user' information affirmatively and through material omissions regarding the privacy protection FB promised to provide.

904. FB willfully and recklessly did not disclose that Plaintiffs' FB user' information could be obtained by numerous third parties.

905. Plaintiffs have suffered significant harm due to FB' deceptive and unfair business acts and practices.

906. Plaintiffs' FB user information has tangible value.

907. FB repeatedly told Plaintiffs that they alone owned their FB user' information.

908. Additionally, because FB directly leveraged unfettered access to Plaintiffs' information in order to obtain revenues from numerous third parties, Plaintiffs have a property interest in FB's profits because FB took Plaintiff's property without compensation.

909. There is value in Plaintiffs' information that FB disseminated to FB business partners, "whitelisted" applications and numerous other third parties as demonstrated by the thirst of third parties and FB for that information.

910. Plaintiffs lost the opportunity to receive value from FB and these third parties in exchange for their FB user' information.

911. Plaintiffs' FB user' information is still in the possession of FB and numerous third parties who have used and will use it for their own advantage, including financial advantage, or have sold it or will sell it for value, making it clear that Plaintiffs' information has tangible value.

912. Plaintiffs are at increased risk of identity theft due to FB's practices concerning sharing users' information with third parties.

913. Plaintiffs may be subjected to future voter fraud, identity theft, medical fraud, and other harms.

914. The information shared with third parties allows this information to be aggregated with other information to identify and target Plaintiffs.

915. FB invaded Plaintiffs' privacy by failing to inform Plaintiffs that FB was sharing their information with numerous third parties, including but not limited to application developers, FB business partners, device manufacturers, mobile carriers, software makers, security firms, banks, credit reporting and government agencies, chip designers, retailers such as Amazon and wholesalers.

916. ' FB did not disclose the nature or the extent of the exploitation of Plaintiffs' FB content and user' information.

917. FB invaded Plaintiffs' privacy by subjecting them to psychographic marketing that exploited intimate aspects of their identity, including emotional and psychological manipulation.

918. Plaintiffs' information was exploited without Plaintiff's informed consent.

919. Accordingly, Plaintiffs are entitled to part of FB's profits that were generated by their information without informed consent.

920. Plaintiffs seek an order to enjoin FB from such unlawful, unfair, and fraudulent business acts or practices, and to restore to Plaintiffs their interest in money or property that may have been acquired by FB by means of unfair competition.

921. Section 17203 of the UCL authorizes a court to issue injunctive relief "as may be necessary to prevent the use or employment by any person of any practice which constitutes unfair competition."

922. Plaintiffs also seek the following injunctive relief: (1) an "opt in" rather than "opt out" default for sharing personal content in all of FB's user settings; (2) disclosure of the purposes of which Plaintiffs' personal content is used by FB, information brokers, device makers, mobile carriers, software makers, security firms, application developers, advertisers and other third parties with whom FB has shared users' information without their consent; (3) destruction of all personal content obtained by FB and all such third parties where such content is within FB' control or possession; (4) a complete audit and

accounting of the uses of Plaintiffs' FB user' information by third parties; (5) a permanent injunction preventing such sharing of information with these third parties without FB users' informed consent and affirmative authorization; and (6) a permanent ban on targeting Plaintiffs with advertisements or marketing materials based on information from information brokers.

XI. PRAYER FOR RELIEF

WHEREFORE, in accord with the above paragraphs and as this Court deems appropriate, Plaintiffs respectfully request the following relief:

923. Plaintiffs request that the Court enter judgment in their favor and against FB Defendants, as follows:

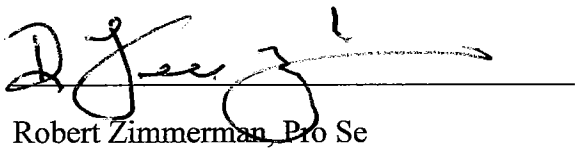
924. Enter Judgment against FB Defendants on Plaintiffs' asserted causes of action and award Plaintiffs appropriate relief, including actual and statutory damages, restitution, disgorgement, and punitive damages, equitable, injunctive, and declaratory relief as may be appropriate.

925. Award all costs, including experts' fees and attorneys' fees, if any, as well as the costs of prosecuting this action; pre-judgment and post-judgment interest as prescribed by law; and grant additional legal and equitable relief as this Court may find just and proper.

XII. DEMAND FOR JURY TRIAL

926. Plaintiffs hereby demand a trial by jury on all the issues so triable.

Respectfully submitted by,



Robert Zimmerman, Pro Se Dated: August 5, 2019